A closer look into a well known quotient ring

(By- Debashish Sharma, Junior Research Fellow, Dept. of Mathematics, NIT Silchar)

The ring $Z[i] = \{a + ib: a, b \in Z, i^2 = -1\}$ is quite a well- known ring in Algebra. Further, being a principal ideal domain, every ideal of $Z[i]$ is generated by a single element say $a + ib \in Z[i]$ and so can be taken in the form $< a + ib > = \{(x + iy)(a + ib): x, y \in Z\}$.

We now consider the quotient ring $Z[i]/< a + ib > = \{(x + iy) + < a + ib >: x, y \in Z\}$ and try to look for a precise way of representing the elements in it. First we suppose that a and b are both non zero. The quantities $d = \gcd(a, b)$ and $N = (\mathrm{a}^2 + \mathrm{b}^2)/\gcd(\mathrm{a}, \mathrm{b})$ deserve special attention in the discussion.

Result A :- An integer $n \in < a + ib >$ if and only if $n \in < (\mathrm{a}^2 + \mathrm{b}^2)/\gcd(\mathrm{a}, \mathrm{b}) >$.

Proof: Since $d = \gcd(a, b)$, we can write $a + ib = d(p + iq)$ where $\gcd(p, q) = 1$.

Now let $n \in < a + ib >$. This implies that $n = (a + ib)(x + iy)$ for some $x + iy \in Z[i]$

$\Longrightarrow n = d(p + iq)(x + iy)$, which gives $py = -qx \Longrightarrow p|qx$ and $q|py$. ("|" means divides)

And since $\gcd(p, q) = 1$, so $p|x$ and $q|y$ which means that x/p and y/q are integers.

Also, $py = -qx \Longrightarrow x/p = -y/q = k$ say, where $k \in Z$.

Thus we get $n = d(p + iq)(kp - ikq)$

$\Longrightarrow n = d(p^2 + q^2)\ (k + i0)$ which shows that $n \in < d(p^2 + q^2) >$.

But $d(p^2 + q^2) = \{(dp)^2 + (dq)^2\}/d = (a^2 + b^2)/\gcd(a, b) = N$. Hence, $n \in < N >$.

Conversely if $n \in < N >$ then by using the relation $a^2 + b^2 = (a + ib)(a - ib)$ it can be easily shown that $n \in < a + ib >$.

Therefore $n \in < a + ib >$ if and only if $n \in < (\mathrm{a}^2 + \mathrm{b}^2)/\gcd(\mathrm{a}, \mathrm{b}) >$ ■

Result B :- For any $n \in Z$, $ni \in < a + ib >$ if and only if $n \in < N >$.

Proof: Similar to above. ■

Observation:

1. Since 1,2, … … , $N - 1$ do not belong to $< a + ib >$ so it is clear that the elements $0 + < a + ib >, 1 + < a + ib >, \ldots \ldots, (N - 1) + < a + ib >$ of $Z[i]/< a + ib >$ are distinct .
2. Since $a^2 + b^2 = (a + ib)(a - ib)$ so it is to be noted that $< N > \subseteq < a + ib >$.
3. If $n \in Z$ then by division algorithm, there exist unique $q, r \in Z$ with $0 \leq r < N$ such that $n = Nq + r$. Since $n - r = Nq \in < a + ib >$ so $n + < a + ib > = r + < a + ib >$.

Thus any element of the form $n + < a + ib >$, where $n \in Z$, can be reduced to the form $r + < a + ib >$ for a unique integer r satisfying $0 \leq r < N$.

The following result is further more generalized :

Result C :- $Z[i]/< a+ib >= \{r+is+< a+ib >: r,s \in Z \text{ and } 0 \le r < N \text{ and } 0 \le s < d\}$.

Proof: The proof is a just a simple application of a well- known property of GCD.

We take any element $x+iy+< a+ib >$ of $Z[i]/< a+ib >$. By division algorithm, we can write $y = qd+s$ where $q,s \in Z, 0 \le s < d$. Again since $d = \gcd(a,b)$ so there exist $u,v \in Z$ such that $d = au+bv$. And it is easy to see that $d = (a+ib)(u-iv) - i(bu-av)$ which gives

$$x+iy+< a+ib > = (x+qbu-qav) + is + iq(a+ib)(u-iv) + < a+ib >$$
$$= (Nw+r) + is + < a+ib >, \text{ where } 0 \le r < N, \quad \text{(division algorithm)}$$
$$= r+is+< a+ib > \text{ where } 0 \le r < N, 0 \le s < d \quad (\because Nw \in < a+ib >)$$

Hence the result ■

Result D :- The elements in the set in RHS of D are distinct.

Proof: Let $A = \{r+is+< a+ib >: r,s \in Z \text{ and } 0 \le r < N \text{ and } 0 \le s < d\}$

Let $x_1+iy_1+< a+ib >$ and $x_2+iy_2+< a+ib >$ be any two members of A.

Since $0 \le y_1, y_2 < d$ and $0 \le x_1, x_2 < N$ a simple observation reveals that

1. $x_1 - x_2$ cannot be a non –zero multiple of N and
2. $y_1 - y_2$ cannot be a non-zero multiple of d.

The above members will be equal if $(x_1+iy_1) - (x_2+iy_2) \in < a+ib >$

ie if $(x_1-x_2) + i(y_1-y_2) \epsilon < a+ib >$

$\Longrightarrow (x_1-x_2) + i(y_1-y_2) = (a+ib)(m+in)$ for some $m,n \in Z$

$\Longrightarrow (x_1-x_2) = am-bn$ and $(y_1-y_2) = bm+an$

$\Longrightarrow d|(x_1-x_2)$ and $d|(y_1-y_2)$ since $d = \gcd(a,b)$

ie $y_1 - y_2$ is a multiple of d but by (1) above $y_1 - y_2 = 0$ *ie* $y_1 = y_2$

We thus have $x_1 - x_2 \, \epsilon < a+ib >$ which in turn implies that $x_1 - x_2$ is a multiple of N but by (2) above, the only possibility is $x_1 - x_2 = 0$ *ie* $x_1 = x_2$ .Thus the elements of A are distinct. ■

Conclusion: From the above results it is clear that

1. $Z[i]/< a+ib > = \{r+is+< a+ib >: r,s \in Z \text{ and } 0 \le r < N \text{ and } 0 \le s < d\}$
2. $Z[i]/< a+ib >$ contains exactly the above $N \times d = a^2+b^2$ elements.
3. If $\gcd(a,b) = 1$, then $Z[i]/< a+ib > = \{x+< a+ib >: 0 \le x < a^2+b^2\}$ which is isomorphic to the ring $Z_{a^2+b^2}$ of integers modulo a^2+b^2.
4. Further if a^2+b^2 is prime then $Z[i]/< a+ib >$ is a field and so $< a+ib >$ is maximal.
5. Another way of representing $Z[i]/< a+ib >$ is
   $Z[i]/< a+ib > = \{r+is+< a+ib >: r,s \in Z \text{ and } 0 \le r < d \text{ and } 0 \le s < N\}$
6. It can be proved that the same result holds for the case when one of a or b is zero. In this case we can take $\gcd(a,0) = |a|$ and $\gcd(0,b) = |b|$).

   There may be other better ways of representing the elements of $Z[i]/< a+ib >$

We can try looking for other such smarter ways !! ■